

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

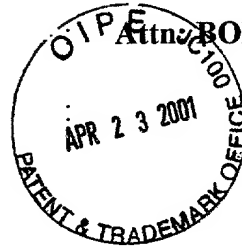
In re application of

Ryuichi OKAMOTO et al.

Serial No. 09/757,578

Filed January 11, 2001

A DATA DISTRIBUTING SYSTEM



Attorney: BOX MISSING PARTS

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEE FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975.

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents,
Washington, D.C.

Sir:

Kindly amend the application as follows:

IN THE SPECIFICATION:

Please replace the paragraph beginning at page 3, line 1, with the following rewritten paragraph:

When the user plays the digital data on the receiving device 102, the digital data administration means 111 reads the encrypted digital data from the storage media 117, and its decryption key from the secure information storage means 112, and decrypts the digital data.

Please replace the paragraph beginning at page 3, line 5, with the following rewritten paragraph:

When the digital data written in the digital data storage means 113 is to be copied to another portable storage media 117, the digital data administration means 111 refers to the use condition information and copy history information that are stored in the secure information storage means 112.

09/757,578

The copy history information indicates the number of copies that have been made in the past. In this manner, the digital data administration means 111 determines whether the digital data may be copied. If the digital data administration means 111 determines that the digital data may be copied, the media access process control means 114 receives the digital data and its decryption key from the digital data administration means 111, and copies them in the storage media 117 via the storage media access means 116. At this time, the decryption key is copied after being encrypted with a media ID 118, which is an ID unique to each storage media 117 and has been detected by the media ID detection means 115. Once the digital data is copied to the storage media 117, the digital data administration means 111 increments the copy history information by one. The copy history information is stored in the secure information storage means 112.

Please replace the paragraph beginning at page 4, line 13, with the following rewritten paragraph:

The tamper-resistant technology is closely related to the structure of a device to which the tamper-resistant technology is applied. Therefore, when there is a plurality of devices which have different structures, a tamper-resistant technology has to be developed for each device. This is a huge burden for manufacturers which develop and sale devices. Also, it is difficult for providers of digital data distribution services to start new services if a tamper-resistant technology has to be developed for each receiving device every time a new service is started in order to let devices having different structures receive the service.

Please replace the paragraph beginning at page 14, line 14, with the following rewritten paragraph:

Figure 2 is a view of an example of application of a digital data distribution system in accordance with the first embodiment of the present invention. 201 is a digital data distribution service firm which operates a distribution server for distributing digital data. 203 is a STB (Set Top

Box) operated by a consumer. 202 is a Cable base station, which connects the digital data distribution service firm 201 and the receiving device 203 of the consumer via a Cable network. 204 is a storage media in which the distributed digital data is written. 205 is an access adapter that is connected to the receiving device 203, and writes in the storage media 204 the digital data that the receiving device 203 receives.

Please replace the paragraph beginning at page 16, line 24, with the following rewritten paragraph:

Figure 8 is a view of an example of the service type database. The service type database includes service ID that is the index information, service name, payment method type for the service, fee for the service, DL (download) song number limit, which is information regarding the limit on the number of songs a user can download, and DL times limit, which is information regarding the limit on the number of times of download per song.

Please replace the paragraph beginning at page 17, line 14, with the following rewritten paragraph:

The history database 307 is a history database that administers information regarding distributions made to users. Figure 11 is a view of its example. The history database 307 includes history ID, which is the index, pertinent right ID, date of the process, type of the process, and DL location media ID.

Please replace the paragraph beginning at page 18, line 18, with the following rewritten paragraph:

The updating control means 314 directs the secure communication method updating means 313 and the secure communication method updating means 325 to update the secure communication

means 312 and the secure communication means 318 and change the method that is utilized to establish the secure communication path between the secure communication means 312 and the secure communication means 318 when, for instance, the method that has been utilized to establish the secure communication path between the secure communication means 312 and the secure communication means 318 is hacked.

Please replace the paragraph beginning at page 24, line 14, with the following rewritten paragraph:

(S1506) The user selects digital data that he wishes to obtain, using the browsing means 316. Then, the browsing means 316 sends the information regarding the selected digital data to the distribution server 301.

Please replace the paragraph beginning at page 25, line 11, with the following rewritten paragraph:

(S1603) The user selects the digital data that he wishes to obtain, using the browsing means 316. The browsing means 316 sends the information regarding the selected digital data to the distribution server 301.

Please replace the paragraph beginning at page 27, line 8, with the following rewritten paragraph:

Figure 18 shows an operational flow of the storage media legitimacy check process. The storage media legitimacy check process is a process in which distribution server 301 checks the legitimacy of the storage media 327 in which the user is about to write the digital data. Its operation will now be explained.

Please replace the paragraph beginning at page 29, line 2, with the following rewritten paragraph:

(S1906) The media access process control means 323 writes the key that the decryption key encryption means 322 has encrypted in S1905 in the secure data area 401 of the storage media 327, by controlling the storage media access means 324.

Please replace the paragraph beginning at page 29, line 6, with the following rewritten paragraph:

(S1907) The media access process control means 323 writes the digital data that the encryption conversion means 321 has encrypted in S1904 in the data area 402 of the storage media 327, by controlling the storage media access means 324.

Please replace the paragraph beginning at page 31, line 17, with the following rewritten paragraph:

(S2704) The media access process control means 323 writes the key that the decryption key encryption means 322 has encrypted in S2703 in the secure data area 401 of the storage media 327, by controlling the storage media access means 324.

Please replace the paragraph beginning at page 31, line 21, with the following rewritten paragraph:

(S2705) The media access process control means 323 writes the digital data that the digital data distribution means 310 has sent in S2701 in the data area 402 of the storage media 327, by controlling the storage media access means 324.

Please replace the paragraph beginning at page 33, line 3, with the following rewritten paragraph:

Figure 29 shows an operational flow of the storage media writing process in accordance with the third embodiment. Its operation will now be explained.

Please replace the paragraph beginning at page 33, line 14, with the following rewritten paragraph:

(S2903) The digital data distribution means 310 sends the decryption key that the decryption key encryption means 322 has encrypted in S2902 to the storage media access adapter 303.

Please replace the paragraph beginning at page 33, line 17, with the following rewritten paragraph:

(S2904) The media access process control means 323 writes in the secure data area 401 of the storage media 327 the decryption key that the digital data distribution means 310 has sent in S2903, by controlling the storage media access means 324.

Please replace the paragraph beginning at page 33, line 21, with the following rewritten paragraph:

(S2905) The media access process control means 323 writes in the data area 402 of the storage media 327 the digital data that the digital data distribution means 310 has sent in S2901, by controlling the storage media access means 324.

IN THE CLAIMS:

Kindly amend claims 4 and 5 as follows:

4.(Amended) A digital distribution control method for controlling distribution of digital data, wherein

in said digital distribution system as set forth in claim 1,

said distribution front end authorizes a user based on said adapter ID sent from said adapter ID detecting means, and

said distribution front end determines whether the digital data with respect to which distribution is requested can be distributed, by referring to said obtained rights administration database, said history database, said digital data administration database, and said storage media administration database, in order to execute processes in response to a request for distribution of digital data from the authorized user.

5.(Amended) The digital data distribution system as set forth in claim 1, wherein

said adapter includes secure communication means updating means for updating said secure communication means of said adapter, and

said distribution server includes

secure communication means updating means for updating said secure communication means of said distribution server, and

secure communication means update direction means for directing said secure communication updating means within said adapter and said secure communication updating means within said distribution server to update said secure communication means.

Kindly add the following new claims:

6.(NEW) A digital distribution control method for controlling distribution of digital data, wherein

in said digital distribution system as set forth in claim 2,
said distribution front end authorizes a user based on said adapter ID sent from said adapter ID detecting means, and

said distribution front end determines whether the digital data with respect to which distribution is requested can be distributed, by referring to said obtained rights administration database, said history database, said digital data administration database, and said storage media administration database, in order to execute processes in response to a request for distribution of digital data from the authorized user.

7.(NEW) A digital distribution control method for controlling distribution of digital data, wherein

in said digital distribution system as set forth in claim 3,

said distribution front end authorizes a user based on said adapter ID sent from said adapter ID detecting means, and

said distribution front end determines whether the digital data with respect to which distribution is requested can be distributed, by referring to said obtained rights administration database, said history database, said digital data administration database, and said storage media administration database, in order to execute processes in response to a request for distribution of digital data from the authorized user.

8.(NEW) The digital data distribution system as set forth in claim 2, wherein
said adapter includes secure communication means updating means for updating said secure communication means of said adapter, and

said distribution server includes

secure communication means updating means for updating said secure communication means of said distribution server, and

secure communication means update direction means for directing said secure communication updating means within said adapter and said secure communication updating means within said distribution server to update said secure communication means.

9.(NEW) The digital data distribution system as set forth in claim 3, wherein
said adapter includes secure communication means updating means for updating said secure communication means of said adapter, and
said distribution server includes
secure communication means updating means for updating said secure communication means of said distribution server, and
secure communication means update direction means for directing said secure communication updating means within said adapter and said secure communication updating means within said distribution server to update said secure communication means.

TOC-134567

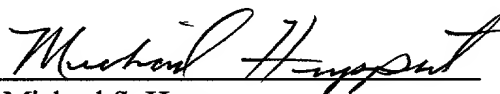
REMARKS

The present Preliminary Amendment is submitted to delete the multiple dependencies of claims 4 and 5, thereby placing such claims in condition for examination and reducing the required PTO filing fee and also amend the specification has been revised in order to make a number of minor clarifying and other editorial amendments.

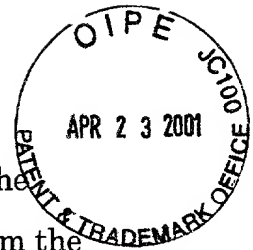
Copies of the amended portion of the specification and claims with changes marked therein are attached and entitled "*Version with Markings to Show Changes Made.*"

Respectfully submitted,

Ryuichi OKAMOTO et al.

By: 
Michael S. Huppert
Registration No. 40,268
Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 23, 2001



1 When the user plays the digital data on the receiving device 102, the digital data administration means 111 reads the encrypted digital data from the storage media ¹¹⁷[113] and its decryption key from the secure information storage means 112, and decrypts the digital data.

5 When the digital data written in the ^{digital data storage means 113}storage media 114 is to be copied to another portable storage media 117, the digital data administration means 111 refers to the use condition information and copy history information that are stored in the secure information storage means 112. The copy history information indicates the number of copies that have been made in the past. In this manner, the digital data administration means 111 determines whether the digital data may be copied. If the digital data administration means 111 determines that the digital data may be copied, the media access process control means 114 receives the digital data and its decryption key from the digital data administration means 111, and copies them in the storage media 117 via the storage media access means 116. At this time, the decryption key is copied after being encrypted with a media ID 118, which is an ID unique to each storage media 117 and has been detected by the media ID detection means 115. Once the digital data is copied to the storage media 117, the digital data administration means 111 increments the copy history information by one. The copy history information is stored in the secure information storage means 112.

As described above, in the conventional technology, the distribution server uses only the user information in order to conduct digital data distribution control. On the other hand, the receiving device administers the decryption key of the digital data, the use right information of the digital data, and the use history information of the digital data with designated secure information storage means 112, which can not be accessed with a consumer's regular operation.

Such conventional digital data distribution system is always subject to

However, the aforesaid conventional structure has following problems, because the equipment of the tamper-resistant technology within the receiving device is indispensable.

13. The tamper-resistant technology is closely related to the structure of a device to which the tamper-resistant technology is applied. Therefore, when there is a plurality of devices which have different structures, a tamper-resistant technology has to be developed for each device. This is a huge burden for manufacturers which develop and sale devices. Also, it is difficult for providers of digital data^{distribution} services to start new services if a tamper-resistant technology has to be developed for each receiving device every time a new service is started in order to let devices having different structures receive the service.

SUMMARY OF THE INVENTION

The present invention has been conceived for the aforementioned situations. More specifically, the object of the present invention is to provide a system in which a plurality of devices having different structures can receive various services without taking into consideration the difference in the structure, by conducting administration of rights of digital data at a server, installing an interface portion to a storage media in an adapter that accesses the storage media,

1 accordance with the second embodiment of the present invention.

Figure 27 is a flowchart explaining a storage media writing process in accordance with the second embodiment of the present invention.

Figure 28 shows a structure of the digital data distribution system in accordance with the third embodiment of the present invention.

Figure 29 is a flowchart explaining a storage media writing process in accordance with the third embodiment of the present invention.

Figure 30 shows an example of the digital data distribution system in accordance with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIRST EMBODIMENT

A first embodiment of the present invention will now be explained referring to figures.

14 Figure 2 is a view of an example of application of a digital data distribution system in accordance with the first embodiment of the present invention. 201 is a digital data distribution service firm which operates a distribution server for distributing digital data. 203 is a STB (Set Top Box) operated by a consumer. 202 is a Cable base station, which connects the digital data distribution service firm 201 and the receiving device 203 of the consumer via a Cable network. 204 is a storage media in which the distributed digital data^{is} written. 205 is an access adapter that is connected to the receiving device 203, and writes in the storage media 204 the digital data that the receiving device 203 receives.

In this embodiment, a situation where the digital data is music digital data is discussed as an example. Also, services provided by the digital data distribution system include three services as examples: single sale service in which each song has a fixed price, a subscription service in which the consumer can freely download any desired songs from a designated group of music digital

Each structural element will now be explained below.

The user administration database 304 is a relational database that includes three databases: a user account information database that stores users' account information, an adapter information database that stores information regarding adapters that users own, and a storage media information database that stores information regarding storage medias that users have used as the distribution location in the past. Figure 5 is a view of an example of the user account information database. The user account information database includes user ID, log-in name, password, user's name, user's address, the type of credit card with which payment is to be made, credit card number, and information regarding the music distribution service plan the user has joined. Figure 6 is a view of an example of the adapter information database. The adapter information database includes an adapter registration ID, which is the index information of this database, user ID of the owner of the adapter, information regarding the type of the adapter, and adapter ID.

Figure 7 is a view of an example of the storage media information database. The storage media information database includes media registration ID, which is index information of this database, user ID which has received distribution of digital data, information regarding type of media, and media ID.

The digital data administration database 305 includes a service type database which stores digital data vending service plans that are sold at the site, and a digital data information database that stores information regarding the digital data itself and information regarding the storage locations of the digital data.

Figure 8 is a view of an example of the service type database. The service type database includes service ID that is the index information, service name, payment method type for the service, fee for the service, DL_(download) song number limit,

| which is information regarding the limit on the number of songs a user can download, and DL times limit, which is information regarding the limit on the number of times of download per song.

Figure 9 is a view of an example of the digital data information database. The digital data information database includes digital data ID, name of digital data song, name of artist, service ID to which the digital data belongs, fee for the digital data, and storage location information of the digital data.

The obtained rights administration database 306 is a database that administers rights to have digital data distributed, that the users have obtained. Figure 10 is a view of its example. The obtained rights administration database 306 includes right ID, which is the index, user ID which has obtained a right to have digital data distributed, digital data ID of the digital data, date of purchasing the right, and service ID to which the digital data belongs.

14 The history database 307 is a history database that administers information regarding distributions made to users. Figure 11 is a view of its example. The history database 307 includes history ID, which is the index, pertinent right ID, date of the process, [content]^{type} of the process, and DL location media ID.

The distribution digital data storage means 308 stores the digital data to be distributed, after encrypting the digital data with a predetermined encryption system. The distributed digital data storage means 308 also stores the decryption key. Hereinafter, the encryption system employed herein is referred to as a first encryption system.

The distribution front end 309 creates homepage screen data of homepages to which the user accesses, and provides the homepage screen data to the user. The distribution front end 309 also executes processes of responding to operations that the user performs on the homepage screen data created by the distribution

front end 309.

The digital data distribution means 310 executes a process of sending the encrypted digital data and the decryption key that are stored in the distribution digital data storage means 308 to the storage means access adapter 303.

The sending and receiving means 311 and the communication means 315 execute a communication process between the distribution server 301 and the receiving device 302. This communication process is executed securely using certain technologies such as SSL (Secure Socket Layer) as needed.

The secure communication means 312 and the secure communication means 318 communicate with each other, thereby establishing a secure communication path between the distribution server 301 and the storage media access adapter 303. Communication between each structural element within the distribution server 301 and each structural element within the storage media access adapter 303 is conducted through this secure communication path.

The secure communication method updating means 313 updates the secure communication means 312 according to a direction from the updating control means 314, which will be described later.

18 The updating control means 314 directs the secure communication method updating means 313 and the secure communication method updating means 325 to update the secure communication means 312 and the secure communication means 318 and change ^{the} ~~their~~ method, ^{that is utilized to establish the secure communication path between} when, for instance, the method that has been utilized to establish the secure communication path between the secure communication means 312 and the secure communication means 318 is hacked. ^{the secure communication means 312 and the secure communication means 318}

The browsing means 316 displays the homepage screen data. The browsing means 316 also receives and processes operations that the user made on the homepage screen data.

The adapter connection control means 317 connects the receiving device

the browsing means 316.

(S1504) If it is determined in S1501 that the user is a member, the distribution front end 309 refers to the obtained rights administration database 306, and determines for each digital data that is included in the selected subscription service whether the user has already obtained the right to download.

(S1505) The distribution front end 309 displays a list of digital data that belong to the selected service according to the digital data administration database 305, such that the user can select digital data that belongs to the selected service. For the digital data with respect to which the right to download has already been obtained, the distribution front end 309 creates screen data in which these digital data bear a mark indicating that the right has already been obtained. The screen data is sent to the user device 302. The browsing means 316 displays the screen. An example of the screen is shown in Figure 22.

(S1506) The user selects digital data that he wishes to obtain, using the browsing means 316. Then, the browsing means 316 sends ^{the information regarding} the selected digital data to the distribution server 301.

(S1507) The distribution front end 309 newly registers in the obtained rights administration database 306, information regarding the digital data with respect to which the right to download has been requested, based on the information that has been sent out in S1506.

The above concludes the explanation of the subscription handling process.

Figure 16 shows an operational flow of the single sale handling process. The single sale handling process is a process in which a user obtains the right to download digital data that is distributed in the single sale service. Its operation will be explained below.

(S1601) The distribution front end 309 refers to the obtained rights administration database 306, and determines for each of digital data that are

included in the single sale service whether the user has obtained right to download.

(S1602) The distribution front end 309 displays a list of digital data that belong to the single sale service according to the digital data administration database 305, such that the user can make a selection. Furthermore, for the digital data with respect to which the user has obtained the right to download as determined in S1601, the distribution front end 309 creates screen data in which these digital data bear a mark indicating that the right has already been obtained. The screen data is sent to the receiving device 302. The browsing means 316 displays the screen. An example of the screen is shown in Figure 23.

\\ (S1603) The user selects the digital data that he wishes to obtain, using the browsing means 316. The browsing means 316 sends the ^{information regarding the} selected digital data to the distribution server 301.

(S1604) The distribution front end 309 calculates the price of digital data with respect to which the user has requested right to download, referring to the digital data administration database 305. Then, a purchasing process is executed using the payment information such as credit card information registered in the user administration database 304.

(S1605) The distribution front end 309 newly registers in the obtained rights administration database 306 the information regarding the digital data for which the purchasing process has been executed.

The above concludes the explanation of the single sale handling process.

Figure 17 shows an operational flow of the digital data download process. The digital data download process is a process in which the user downloads digital data. Its operation will be described below.

(S1701) First of all, the distribution front end 309 obtains from the obtained rights administration database 306 a list of digital data with respect to

storage media may be illegitimate. The screen data is sent to the receiving device 302. The browsing means 316 displays the screen.

(S1709) If it is determined that the storage media 327 is legitimate in S1707, a storage media writing process, which will be described later, is executed.

(S1710) Lastly, the distribution front end 309 adds to the history database 307 the information that the digital data has been downloaded.

The above concludes the explanation of the digital data download process.

Figure 18 shows an operational flow of the storage media legitimacy check process. The storage media legitimacy check process is a process in which a user checks the legitimacy of the storage media 327 in which the user is about to write the digital data. Its operation will now be explained.

(S1801) The distribution front end 309 verifies whether the media ID 328 that has been sent in S1705 is registered in the storage media registration database of the user administration database 304. If the distribution front end 309 determines that the media ID 328 is registered, the system proceeds to S1805.

(S1802) If it is determined in S1801 that the media ID 328 is not registered, the distribution front end 309 detects from the storage media information database of the user administration database 304 the number of storage medias 327 that the same user has used. Then, the distribution front end 309 determines whether the number of the storage medias 327 is greater than a predetermined number.

(S1803) If it is determined in S1802 that the number of the storage medias 327 is greater than the predetermined number, the distribution front end 309 determines that the storage media 327 being checked is not legitimate.

(S1804) If it is determined in S1802 that the number of the storage medias 327 is not greater than the predetermined number, the distribution front end 309 adds the media ID 328 that has been sent in S1705 in the storage media

detected.

2 (S1906) The media access process control means 323 ^{writes} ~~stores~~ the key that the decryption key encryption means 322 has encrypted in S1905 in the secure data area 401 of the storage media 327, by controlling the storage media access means 324.

3 (S1907) The media access process control means 323 ^{writes} ~~stores~~ the digital data that the encryption conversion means 321 has encrypted in S1904 in the data area 402 of the storage media 327, by controlling the storage media access means 324.

This concludes the explanation of the storage media writing process.

Figure 25 shows an operational flow of the secure communication method updating process. The secure communication method updating process is a process in which the secure communication means 312 and the secure communication means 318 are updated in order to renew the method that has been utilized to establish a communication path between the secure communication means 312 and the secure communication means 318 when the method is hacked. Its operation will now be explained.

(S2501) The updating control means 314 directs the secure communication method updating means 313 to update the secure communication means 312. The updating means also directs the secure communication means updating means 325 to update the secure communication means 318. The direction for updating can be conducted by sending a predetermined command, or by sending a software for updating.

(S2502) The secure communication method updating means 313 updates the secure communication means 312. The secure communication method updating means 325 updates the secure communication means 318.

The above concludes the description of the secure communication method

encryption system, and the decryption key that has been encrypted by the decryption key encryption means 322.

Figure 27 shows an operational flow of the storage media writing process according to the second embodiment. Its operation will now be explained.

(S2701) The digital data distribution means 310 sends to the storage media access adapter 303 the digital data which is stored in the distribution digital data storage means 308, and with respect to which a request for downloading has been made.

(S2702) The digital data distribution means 310 sends to the storage media access adapter 303 the decryption key for the digital data, which is stored in the distribution digital data storage means 308, and with respect to which a request for downloading has been made.

(S2703) The decryption key encryption means 322 encrypts the decryption key that the digital data distribution means 310 has sent in S2702, using the media ID 328 that has been detected by the media ID detecting means 320.

17 (S2704) The media access process control means 323 ^{writes} stores the key that the decryption key encryption means 322 has encrypted in S2703 in the secure data area 401 of the storage media 327, by controlling the storage media access means 324.

21 (S2705) The media access process control means 323 ^{writes} stores the digital data that the digital data distribution means 310 has sent in S2701 in the data area 402 of the storage media 327, by controlling the storage media access means 324.

This concludes the explanation of the storage media writing process of the second embodiment. The processes other than the storage media writing process are the same as those in the first embodiment.

from the digital data distribution means 310, by controlling the storage media access means 324.

3 Figure 29 shows an operational flow of the storage media writing process in accordance with the ~~second~~^{third} embodiment. Its operation will now be explained.

(S2901) The digital data distribution means 310 sends to the storage media access adapter 303 the digital data which is stored in the distribution digital data storage means 308, and with respect to which a request for downloading has been made.

(S2902) The decryption key encryption means 322 encrypts the decryption key stored in the digital data storage means 308, using the media ID 328 sent from the media ID detecting means 320. The decryption key corresponds to the digital data with respect to which a request for downloading has been made.

14 ^{S2903}
~~(S2703)~~ The digital data distribution means 310 sends the decryption key that the decryption key encryption means 322 has encrypted in S2902 to the storage media access adapter 303.

17 (S2904) The media access process control means 323 ^{writes} stores in the secure data area 401 of the storage media 327 the decryption key that the digital data distribution means 310 has sent in ^{S2903} ~~(S2703)~~, by controlling the storage media access means 324.

21 ^{S2905}
~~(S2705)~~ The media access process control means 323 ^{writes} stores in the data area 402 of the storage media 327 the digital data that the digital data distribution means 310 has sent in ^{S2901} ~~(S2701)~~, by controlling the storage media access means 324.

This concludes the explanation of the storage media writing process of the third embodiment.

Although digital data is music data in the first through third embodiments,